

Field		Content
1	CERTIFICATE SERIAL NUMBER	UP TO THE MANUFACTURER. Eg. THE DEVICE SERIAL NUMBER (ICC ID) COMBINED WITH A KEY NUMBER.
	ISSUER	MANUFACTURER IDENTIFICATION. Eg. THE SAME VALUE AS IN PKCS15TOKENINFO.MANUFACTURERID
	VALID NOT BEFORE	DATE AND TIME OF CREATING/STORING THE KEY AND CERTIFICATE
2	VALID NOT AFTER	END OF EXPECTED MAXIMUM LIFETIME OF THE DEVICE
3	SUBJECT	A CONCENTRATION (STORED AS PRINTABLE STRING) OF • SERIAL NUMBER (ICC ID), SAME AS PKC215TOKENINFO.SERIALNUMBER • A LETTER (OR COMBINATION OF LETTERS) INDICATING KEY USAGE (PRECEDED WITH '-') • OPTIONALLY KEY ORIGINAL NUMBER (PRECEDED WITH '-') Eg. 1234567890123456789-SD-2 9876543210987654-N
4	PUBLIC KEY	PUBLIC KEY ASSOCIATED WITH THE PRIVATE KEY IN THE DEVICE

FIG. 1a

KEY USAGE INDICATOR	SUPPORTED WIM PRIMITIVES WITH THIS KEY	COMMENT
5 N	COMPUTERDIGITALSIGNATURE	NON-REPUDIATION. THE WIM REQUIRES USER VERIFICATION (PIN) EVERY TIME
6 S	COMPUTERDIGITALSIGNATURE	DIGITAL SIGNATURES USED FOR AUTHENTICATION (E.g. FOR WTLS RSA OR SSL HANDSHAKE)
7 K	KEYAGREEMENT	USED IN ECDH HANDSHAKE
8 D	DECIPHER	USED FOR UNWRAPPING A KEY (E.g. FOR S/MIME DECRYPTION)

FIG. 1b

09597982 " 0151900

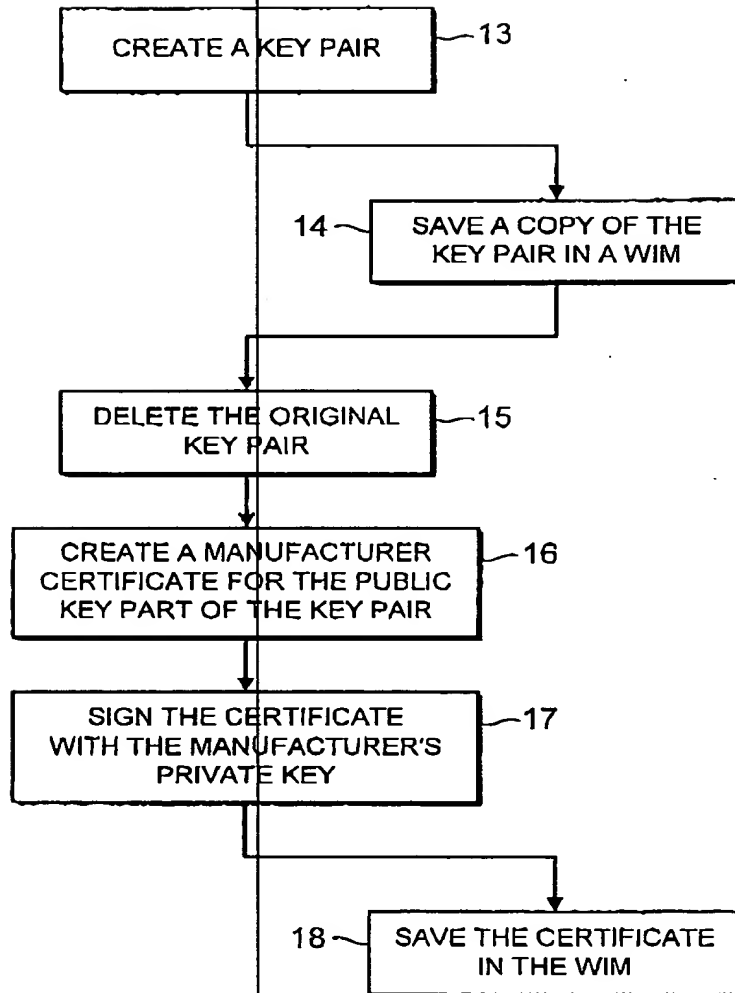


FIG. 2

09597982.06.1900

3 / 3

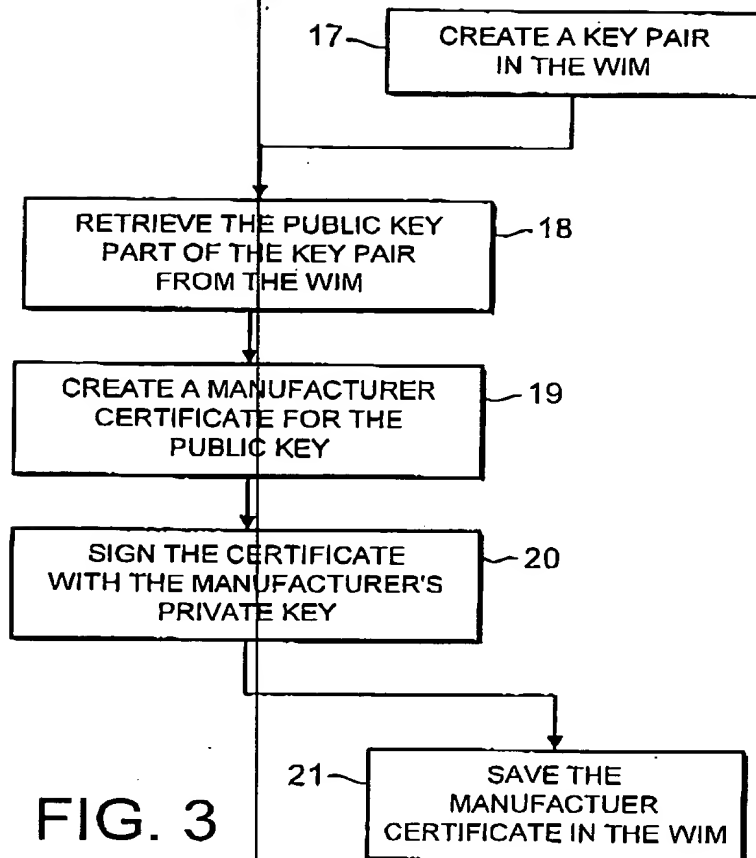


FIG. 3

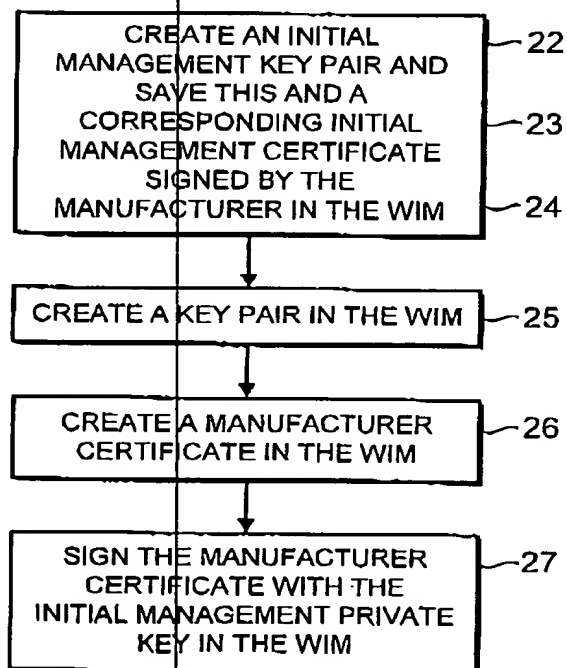


FIG. 4

09597982-061900